ランダムネットワークを用いた誤り訂正符号化法(基研研究会「ニューラルネットワーク〜これからの統計力学的アプローチ〜」,研究会報告)

AUTHOR(S):

樺島, 祥介

ランダムネットワークを用いた誤り訂正符号化法

樺島 祥介 東京工業大学大学院総合理工学研究科

1 はじめに

誤り訂正符号化 (error correcting code) とはノイズが存在する伝達経路を用いて情報伝達を行なわなければならない状況下で、可能な限り正確に情報を伝えるための符号化技法である。一般社会への計算機ネットワーク、情報通信機器の急速な浸透により実社会におけるこの技術の重要性は今後更に増すものと予想される。さて、意外なことに、この技法は統計力学におけるスピングラスモデルの基底状態探索と密接な関係がある。本研究では従来のスピングラス理論で得られた成果をヒントに希釈スピングラスモデルを応用した新しい誤り訂正符号化法を提案し、その性質を統計力学を用いて調べた。

2 誤り訂正符号化

以下、次のような状況を想定する。送るべきメッセージが長さ Nの二値ベクトル$\boldsymbol{\xi} = (\xi_1, \xi_2, \cdots \xi_N)$ (ただし、$\xi_i = \pm 1\ i = 1, \cdots, N$) のように表現されているとする。これを各成分あたり確率pで値が独立に反転してしまう伝送路 (binary symmetric channel, 以下 BSC と呼ぶ) を通じて送信する。そのため、このままでは受信者は各成分あたり確率 $1-p$ でしか正しい情報を受信することが出来ない。

そのような場合、$\boldsymbol{\xi}$ をそれよりも長い長さ Pのベクトル$\boldsymbol{J} = (J_1, J_2, \cdots, J_P)$ $(P > N)$ に変換して (符号化) 送信し、その後受信したメッセージからもとのメッセージを復元する (復号化) ことによりノイズによる誤りを少なくする工夫がしばしばなされる。この種の技法を一般に誤り訂正符号と呼ぶ。では、具体的にどのような手続きで符号化／復号化を行なえば最も効率が良く、またそうすることでどの程度ノイズの影響を押えることが出来るのであろうか？

この問題に対し、Shannon は今から５０年前におよそ次のような内容の定理を証明した [1]。

シャノン限界 (**Shannon's bound**): 符　号化の冗長度を符号化率 $R \equiv N/P$ で定義する。このとき、伝送路の性質で決まるある有限の臨界値 $R_c > 0$ が存在し、$R < R_c$ ならば１ビットあたりの誤り率をゼロにするような符号化法が存在する。例えば BSC の場合

$$R_c = 1 + p\log_2 p + (1-p)\log_2(1-p), \quad (1)$$

である。

これは、一見不思議であるが、たとえ有限の大きさのノイズが存在したとしても、もとのメッセージと同じオーダーの長さの符号に符号化して送信することによってその影響を限りなく小さくできることを意味する。ただし、残念ながら彼の証明は構成的ではなくシャノン限界を達成する実用的な符号化法は未だ発見されていない。

3 Sourlas コード

８０年代末、Sourlas (1989) は実用的誤り訂正符号化法の一つであるパリティチェックコードとスピングラスモデルの基底状態探索と等価性を指摘し、以下のハミルトニアンの最小化に基づく符号化法を提案した。

$$\mathcal{H} = -\sum_{\mu=1}^{P} J_\mu S_{i_{1,\mu}} S_{i_{2,\mu}} \cdots S_{i_{K,\mu}}. \quad (2)$$

ここで、$J_\mu = \xi_{i_{1,\mu}} \xi_{i_{2,\mu}} \cdots \xi_{i_{K,\mu}}$ がメッセージ$\boldsymbol{\xi} = (\xi_1, \xi_2, \cdots, \xi_N)$ から変換され、送信される “符号語”(code word) であり、ハミルトニアン (2) の基底状態を復号化されたメッセージとする。

ノイズが存在しない場合には、もとのメッセージ $\boldsymbol{\xi}^0 = (\xi_1^0, \xi_2^0, \cdots, \xi_N^0)$ が式 (2) を最小化するのは明らかである。また、ノイズが存在する場合もスピン系の強磁性的性質からノイズがある程度の大きさになるまでは基底状態はもとのメッセージの近傍に留まることが期待される。Sourlas はそれまでに得られていたスピングラスモデルの性質を用いて彼の符号化の性能を調べた。その結果、驚くべきことにランダムエネルギーモデル (REM) と呼ばれる $K \to \infty$ の極限のモデルはシャノン限界を満たす符号化法であることが明らかになった。

ただし、彼の議論は全スピンが他の全てのスピンと結合するいわゆる無限次元モデルに基づいているため符号長が $O(N^K)$ 非常に長くその代わりにノイズが非常に大きい

$$R \to 0, \quad p \to 1/2, \quad (3)$$

という非現実的な状況を仮定している。そのため、従来 Sourlas 符号は実用的符号化法とは考えて来られなかった。

4 K/Cコード

Sourlas 符号をヒントに符号化率 Rが有限の実用的符号を構成することを考えよう。有限の符号化率 Rを持つ符号を構成するため Sourlas 符号のようにすべての組合せの $J_{<i_1 i_2 \cdots i_K>}$ を送るのではなく、以下の条件に従って “間引き” して送信する。

- 各符号 J_μはメッセージ$\boldsymbol{\xi} = (\xi_1, \xi_2, \cdots, \xi_N)$ のうちからランダムに抜き出された K個の成分の積である。
- ただし、ハミルトニアン (2) を構成したとき各添字 i $(i = 1, 2, \cdots, N)$ は必ず固定された自然数 C回づつ現れるようにする。

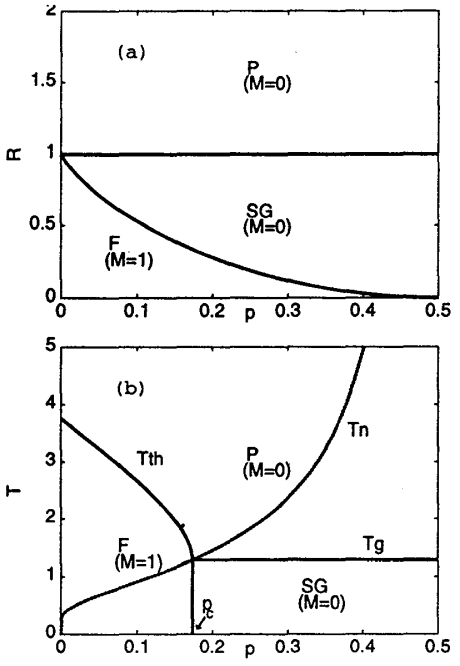

図 1: (a)REM 極限における温度ゼロでの相図。強磁性相とスピングラス相の相境界がシャノン限界に対応する。(b)$\alpha = 1/R = 3$ での有限温度の相図。常磁性相と強磁性相の相境界 T_{th} および常磁性相とスピングラス相の相境界 T_g の交点を西森温度 $T_n = 1/\ln[(1-p)/p]$ が通過することがわかる。

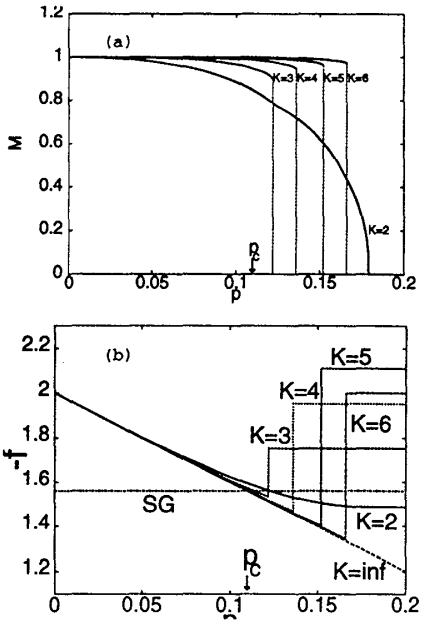

図 2: (a)$K = 2,3,4,5,6$ に対してレプリカ法から得られたオーバーラップの理論値。(b) 対応する自由エネルギーの値。$K \geq 3$ の強磁性が消失した後に転移するスピングラス相は低い自由エネルギー ($-f$は大きい) を持っているがエントロピーが負であるため非物理的な解である。

このような符号化の構成は一見複雑な拘束条件を伴い困難であるように見える。しかしながら、これは各要素が0または1である以下の条件を満たす $N \times P$ の非常にスパースなランダム行列 $\boldsymbol{\Sigma}$ を一旦作っておけば後はそれを用いて簡単に符号 J_μ を作ることが出来る。

- 各行について1となる要素数は K でそれ以外の要素は0。
- 各列について1となる要素数は C でそれ以外の要素は0。

1を取る要素の数に関する保存則から

$$P = N \times C/K, \tag{4}$$

でなければならないことがわかる。この条件を厳密に満足する行列を作ることは難しいが、$O(1)$ 程度の要素は条件を満足しなくて良いことにすると簡単に求められる。$N \to \infty$ の極限を考えるとこの条件緩和の影響は無視することができる。

$\boldsymbol{\Sigma}$ を用いてもとのメッセージ $\boldsymbol{\xi}$ から符号 J_μ を構成するためには $\boldsymbol{\Sigma}$ の μ 行目で1になっている要素の添字に対応する $\boldsymbol{\xi}$ の要素をすべて掛け合わせたものを J_μ とすればよい。この操作に要する時間は $\boldsymbol{\Sigma}$ の1をとる要素を構造体として表現しておけばそれらに関する積操作のみですむので $O(P \times K)$ である。式 (4) より、このことは有限の K, C に対してはメッセージの長さ N に関して $O(N)$ 程度という短時間で符号化が行なえることを意味する。また、その結果得られる符号の符号化率は式 (4) より

$$R = N/P = K/C, \tag{5}$$

である。

この符号化の族を K/C コードと呼ぶことにする。このコードの性能を統計力学を用いて解析すると (詳細は [3]) 自由エネルギーは最終的に

$$\begin{aligned}
&\frac{1}{N}\left\langle\left\langle \ln \mathcal{Z}\right\rangle_J\right\rangle_\xi = \frac{C}{K}\ln\cosh\beta \\
&+\frac{C}{K}\int\left[\prod_{l=1}^{K} dx_l\ \pi(x_l)\right] \\
&\times\left\langle \ln\left[1+\tanh\beta J\ \prod_{j=1}^{K}\tanh\beta x_j\right]\right\rangle_J \\
&-C\int dx\ dy\ \pi(x)\ \hat{\pi}(y)\ \ln\left[1+\tanh\beta x\ \tanh\beta y\right]+ \\
&\int\left[\prod_{l=1}^{C} dy_l\ \hat{\pi}(y_l)\right]\left\langle \ln\left[2\cosh\beta\left(\sum_{j=1}^{C} y_j + F\xi\right)\right]\right\rangle_\xi \\
&-C\int dy\ \hat{\pi}(y)\ \ln\cosh\beta y\ .
\end{aligned}$$

となる。これから得られる "オーダーパラメータ関数" $\pi(x)$、$\hat{\pi}(y)$ の鞍点方程式を解くことで系のマク

ロな性質を調べることができる。その結果、以下のことが明らかになった。

- 符号化率 $R = K/C = 1/\alpha$ を $O(1)$ に保ちながら $K, C \to \infty$(ただし、$K, C << N$) とした REM 極限でこの符号化は大域的に シャノン 限界 (1) を達成する (図 1)。
- ただし、ハミルトニアン (2) に基づく復号化は NP-hard な離散最適化問題である。この種の問題の近似解法として模擬徐冷法が広く知られているが残念ながらこれは REM 極限で非常に困難になる。
- Kに関して $K \to \infty$ の極限への収束はそれほど遅くない。数値的に得られた解の振る舞いを見ると $K \sim 5$ 程度で REM 極限とかなり近い性能を持っている。
- 強磁性相 (符号化が成功する相) ／スピングラス相 (符号化が失敗する相) の転移は $K = 2$ の場合 2 次、$K \geq$の場合 1 次である。すなわち、系の性質は $K = 2$ と $K \geq 3$ で定性的に異なる (図 2)。
- Bethe 近似の一種である TAP 方程式を用いた復号化を提案し実験的にその良好性を確認した [4]。特にメッセージそのものを+1、あるいは−1 のどちらかが出やすくなるように偏らせておくバイアスコーディングを用いた場合、実効的な性能を落すことなく復号化を容易にすることができる (図 3)。

また、現在引続き i) Gaussian channel などの他の種類のノイズに対する性能の検討、ii)Q-clock Potts モデル等を用いた multi-state コーディング、iii) MN コード、Gallager コード、turbo コードなど他の符号化法への統計力学的解析の適用、iv)TAP 方程式のダイナミクスの理論的解析、v)TAP 方程式の情報幾何学的意味付けなどの研究を行っている。

参考文献

[1] C.E. Shannon, *Bell Sys. Tech. J.*, **27**, 379 (1948); **27**, 623 (1948).

[2] N. Sourlas, *Nature*, **339**, 693 (1989).

[3] Y. Kabashima and D. Saad, "Statistical Mechanics of Error Correcting Codes", *preprint* (1997).

[4] Y. Kabashima and D. Saad, "Belief propagation vs. TAP for decoding corrupted messages", *preprint* (1998).

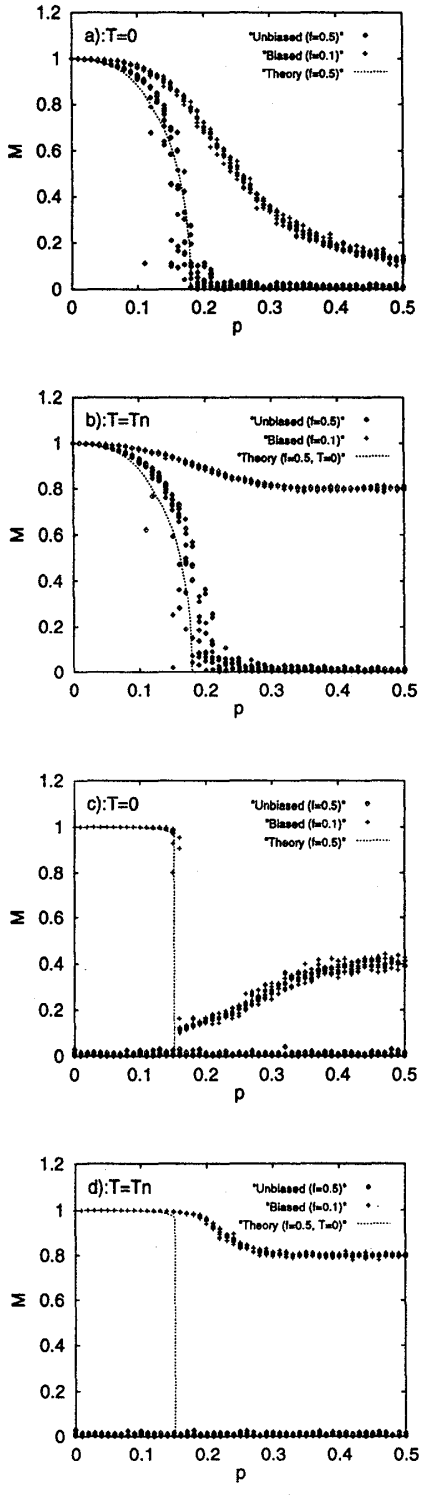

図 3: (a)$K = 2, T = 0$、(b)$K = 2, T = T_n$、(c)$K = 5, T = 0$、(d)$K = 5, T = T_n$ でバイアスコーディングを行なった場合 ($f_+ = 0.1$) と行なわなかった場合 ($f_+ = 0.5$) に TAP 方程式を用いて得られた復号化の性能。全て $N = 10000$、$R = 1/2$ である。横軸は伝送ノイズの大きさ p、縦軸は磁化、すなわちベイズ最適な復号化で得られたメッセージの推定値と送信したメッセージとのオーバーラップ。